

A Simulation-based Approach to Acquire Information Security Baseline of Network Device

Liu Qi^{1,3}, Shi Zhan^{*2}, Yu Xiao^{1,3}, Huang Jie⁴, Xie Yangjun², Qin Zhe⁵, Wang Juan²

¹Hubei Electric Power Research Institute, Wuhan 430077, China

²School of Computer, Wuhan University, Wuhan 430072, Hubei, China

³Key Laboratory of High-voltage Field-test Technique of SGCC, Wuhan 430077, China

⁴State Grid Hubei Electric Power Company, Wuhan 430074, China

⁵Nsfocus Information Technology Co., LTD

*shizhan204@163.com

Abstract

Because of the rapid development of attack technology, the security problems of information assets are more serious. Security baseline monitoring and management is an important way to protect information assets. In this paper, we proposed an approach to acquiring information security baseline values of network devices through Secure Shell (SSH)/telnet simulation. Moreover, we implemented a security baseline acquisition system for network device based on the approach. Our approach can easily acquire the required security policy and properties of network device, so network administrator can monitor the configuration of network device and eliminate the security risk due to unqualified configuration.

Keywords

Security Baseline; Simulation; Acquisition; Policy; Monitor

Introduction

The security of information assets is highly important for enterprises. However, information assets of enterprises are now under increasing security risks. An important reason causing the problem is that IT manager does not configure and manage system according to the required security strategy, which results in information system's being easy to be attacked. Hence it is vital to establish an information security baseline monitoring and management system to protect the security of enterprise information system (Richard Power and Dario Forte, 2008).

Information security baseline monitoring and management system collects configuration data of all the network devices, hosts, databases in real time, then finds and evaluates risk of information assets by checking policy

compliance between the real-time security configuration and security baseline. Collecting security baseline is the first step of implementing a security baseline monitoring and management system. It is very important for identifying and evaluation of security risk. Security baseline is the minimum security guarantee of information system and the basic security requirement of information system (Tong Liu, 2000)

The security baseline acquisition of network device is difficult because we cannot install program on the network device to collect data. The current security baseline acquisition system mainly uses Simple Network Management Protocol (SNMP) protocol to get configuration information of network device. But the approach based on SNMP just can get a small part of information because of the restriction of the SNMP protocol and its permission. Aiming at the above problem, we proposed a security baseline acquisition approach based on SSH/telnet simulation. Our approach can simulate terminal to connect with network devices, access to data of the network devices, and then process the related data with semantic analysis to get final security baseline values. The advantage of our approach can get the same permissions as super users, and then can obtain all the required security configuration information by executing the corresponding command.

Related Work

Yong Xu (2011) presented a process of building information security baseline system. Chen Li et al. (2009) proposed the importance of making use of

security baseline control to eliminate security risk. Jing Zhou (2011) proposed a way to collect configuration information of the network devices. Security baseline monitoring system can use an authorized user account to collect the security configuration through an open port. The core function of the security baseline monitoring system was to connect with the device and execute acquisition commands on the device.

The most relevant research with our work was (Zhihua CHEN, 2013) to present an idea about how to collect the security data of the network devices. First login the IT device via SSH or telnet, then run the commands to collect the device configuration including the account management of device and security condition. But they did not give an approach of implementation and how to deal with the configuration data to get the final security baseline values.

Our Approach

Design Framework

Telnet is a member of TCP/IP protocols which is a standard protocol and main way of Internet remote login service. Using telnet protocol, we can make a local computer into a terminal of the remote host system. SSH is a security protocol which is more inclined to security, aiming at solving the problem of information clear transmission on the Internet. Through using SSH, you can encrypt all the transmission data, so that man-in-the-middle attack cannot be achieved, and also to prevent DNS spoofs and IP spoofing.

Nowadays, many enterprise information systems disable telnet in consideration of security. Moreover, many old devices only support telnet and do not support SSH. Hence, both SSH simulation and Telnet simulation should be considered for design of security baseline acquisition system.

We presented an approach to collect the security baseline values based on SSH/telnet simulation. We simulated login network devices through SSH/telnet as super users, so we can get almost all required data. Firstly, we simulated as a remote terminal device to login network devices. Then management commands can be inputted in a telnet program. These commands would run just like inputting in a super terminal, so they can control the network devices in local. Furthermore, we can collect security-related data and process the security-related data with semantic

analysis to get the final security baseline values.

The entire collection framework consists of four modules: the module of Acquisition agent, the module of Network devices, the module of processing the data, the module of Acquisition system.

Fig. 1 shows the Framework and Process of Security Baseline Acquisition.

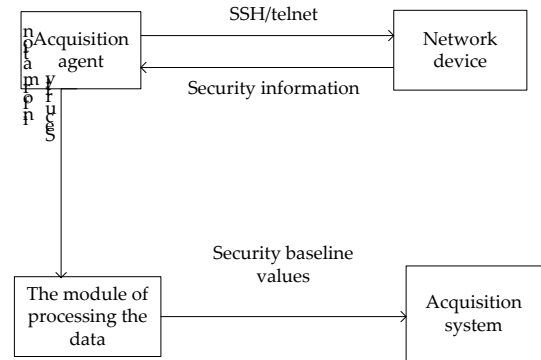


FIG. 1 THE FRAMEWORK AND PROCESS OF SECURITY BASELINE ACQUISITION

Algorithm

Simulate logging the network devices through telnet. The method through SSH was almost the same except the function of establishing connection with the network devices.

① Create a telnet session and connect to the network devices.

This step was to connect the acquisition agent with the network devices through telnet.

② Login the network devices with a username and password.

Build an administrator account to login the network devices.

③ Read commands from a file to the telnet program and execute the commands (such as show version, show run, show SNMP and etc). Use different instructions to collect different devices.

④ Write output results from the telnet program to a file.

⑤ Create a filter instance, match the security data of the network devices with keywords of security baseline values and get the security baseline information.

The core pseudo-code is as following:

Algorithm 1 acquisition

```

1: telnet. Connect (ip, port);
2: in = telnet. getInputStream();
3: out= telnet. getOutputStream();
4: login (user, password);
5: Write command:
6 :( value: show version, show snmp, etc)
7: out. println(value);
8: out. Flush ();
9: Output result:
10:ch = (char) in. read ();
11: While ch!= Endmark
12: ch=(char) in. read ();
13: System .out. Print (ch);
14: output. write(ch);
15: output. flush();
16: End While
17: Input: Security information, keywords
18: For i ←0 to keyw ords. Length
19: For row in Security information
20: If row contains keywords[i]
21: Output: Key ←keyw ords[i]
22: results ←matching result after
23: with keywords[i]
24: End For
25: Iterator<Map. Entry<String, String>>
26: item = results. entrySet().iterator();
27: While item. Has Next ()
28: Map. Entry<String, String> entries =
29: item. next ();
30: Output:
31: key: entries. Get Key ()
32: value: entries. Get Value ();
33: End While

```

Finally we get the security baseline values.

Implementation and Evaluation

We implemented a security baseline acquisition agent based on our approach using Java language. For telnet simulation, we used TelnetClient, a class inherited from org. apache. commons. net. SocketClient, to connect with the network devices. Then input and output flows were obtained through methods of getInputStream and getOutputStream. By executing

corresponding management commands such as (show version, show run, show SNMP and etc), the acquisition agent can get information of the network devices.

For SSH simulation, we used Ganymed SSH-2, which was a common method for simulating logging the network devices through SSH, to connect with the network device. Ganymed SSH-2 is a library which implements the SSH-2 protocol in pure Java.

For evaluating the effectiveness and performance of the security baseline acquisition agent, we used it to connect with a Cisco 2950 device. The security baseline values needed to monitor include four items. First item was network device identifier which should be unique. The second item was password policy which prohibited plaintext password. The third item was ports information. Some needless port should be closed. The fourth item was limiting the management address of SNMP. Through the security baseline acquisition agent, we can collect the above security baseline values of network device identifier and community control field; we can also verify the password policy and port setting policy.

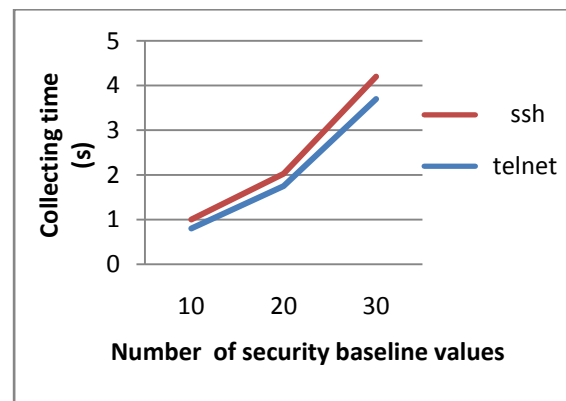


FIG. 2 PERFORMANCE OF SSH /TELNET SIMULATION

Taking account of the number of the devices in some large enterprises was very huge, so we evaluated the performance of the security baseline acquisition agent. After multiple testing, we had figured out the average time of collecting Cisco switch via telnet was 3920 ms while the average time of collecting Cisco switch via SSH was 4000ms. Because SSH needed to decrypt and encrypt instruction in the process of establishing connection and command transmission, it would take more time than telnet. But the security baseline acquisition agent can use special accounts, so it can not affect the running of network device. Hence, the time cost is acceptable in practice. Fig. 2 shows performances of SSH/telnet Simulation.

Conclusion

In this paper, we proposed a security baseline acquisition strategy which was based on simulation. Our work focused on how to connect with the network devices, how to collect the security-related data and how to deal with the security-related data to get the final security baseline values. Our approach can simulate terminal to connect with network devices, access to data of the network devices, and then process the related data with semantic analysis to get final security baseline values. The advantage of our approach can get the same permissions as super users, and then can obtain all the required security configuration information by executing the corresponding command.

REFERENCES

Chen Li, Wei Wang. "The application of security baseline control in the risk management process." *Network*

Security Technology & Application, pp. 4-8, Mar, 2009.

Jing Zhou. "Study and Implementation of Dispatch Gateway Based on Security Baseline Inspection Platform." Master Thesis, 2011

Richard Power and Dario Forte. "Security baselines to give you momentum as you move into the New Year." *Computer Fraud and Security*, v 2008, n 1, p 13-20, January 2008.

Tong Liu. "Study on constructing the complex security baseline of information system." *Chinese Journal of Management Science*, pp. 637-644, Nov 8, 2000.

Yong Xu. "The analysis and design of security baseline evaluation system." Master Thesis, 2011.

Zhihua CHEN. "The applications of security baseline management in the enterprise." *Computer Security*, pp. 19-23, Mar, 2013